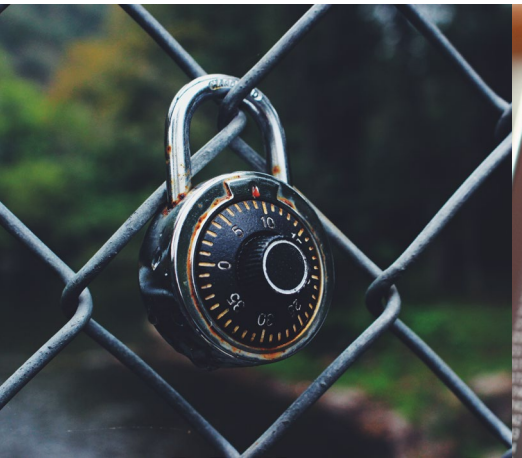
9. Autenticación

Proceso

100%




Índice

9.1. VALIDACIÓN DE IDENTIFICACIÓN EN REDES


Conceptos básicos
Haz clic sobre la pantalla
MacBook Pro

Antes de nada, deberíamos comprender las **diferencias entre:**

Haz clic sobre los círculos

Autenticación

Verifica si algo es auténtico.

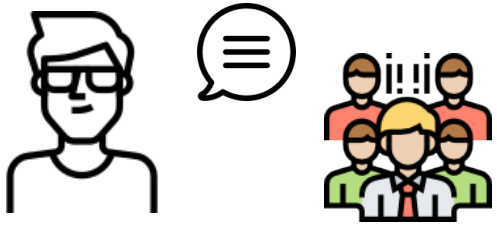
El sistema autentica al usuario en el momento de la conexión comprobando que la contraseña proporcionada es correcta.

Autentificación

Proceso por el que se **comprueba que la persona con la que estamos manteniendo la comunicación es la que debería ser y que no se trata de alguien haciéndose pasar por ella.** Se basa en un elemento de prueba como una clave secreta o pública, lo que **permite asegurarse con un nivel de confianza razonable de la identidad del usuario.**

Al contrario de lo que podría parecer a simple vista, este **tipo de validación es bastante compleja y necesita de protocolos complicados basados en la criptografía.**

Imagina



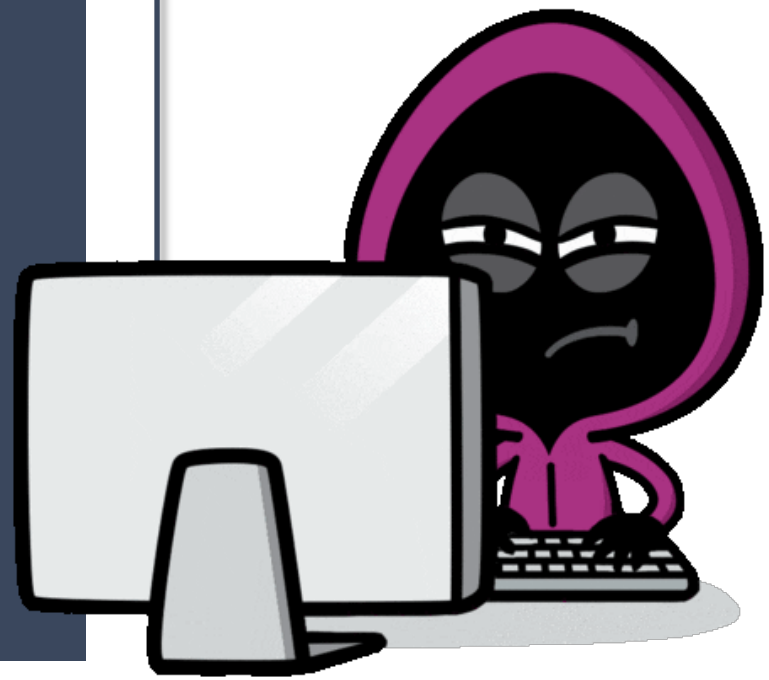
Un usuario empieza generando una comunicación con otro usuario o con un centro de distribución de claves, tras lo que surge un intercambio de mensajes.

Sin embargo, un intruso decide entrar en la comunicación para romperla desde dentro, modificando mensajes y engañando a los usuarios.

Un **protocolo de autenticación** impediría al intruso entrar en la comunicación, lo que generaría y/o mejoraría la seguridad y fiabilidad en la misma.

No es extraño pensar que **una tercera persona se pueda intentar meter en una comunicación ajena**. Cuando una plataforma está diseñada para que varios usuarios hagan uso de ella de forma bidireccional, aumenta la posibilidad de que personas ajenas traten de acceder para extraer beneficios de ella.

Los elementos de validación de identidad y el control de accesos, por lo tanto, se convierten en una alternativa clave para maximizar la seguridad del sistema y la información que en él se maneja.



El *Single Sign-On* o Inicio de Sesión Único

Se ha convertido en uno de los mejores **métodos de autenticación**, que permite acceder a varios sistemas identificándote una sola vez. Esto logra que una autenticación contra el mismo se extienda inmediatamente al resto de aplicaciones.

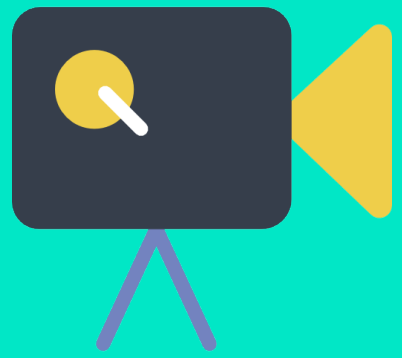
Características

Haz clic sobre el botón

Características

- Cuenta con un **sistema de confianza** que otorga las identidades y gestiona la información.
- Tiene un **proveedor de servicios** que aprueba las credenciales.
- El **propietario** del recurso **gestiona los permisos de acceso**.
- Un **agente usuario representado** por una identidad del sistema.

9.2. VALIDACIÓN DE IDENTIFICACIÓN EN REDES: MÉTODOS DE AUTENTICACIÓN



A continuación, recordamos qué es la autenticación.

AUTENTICACIÓN

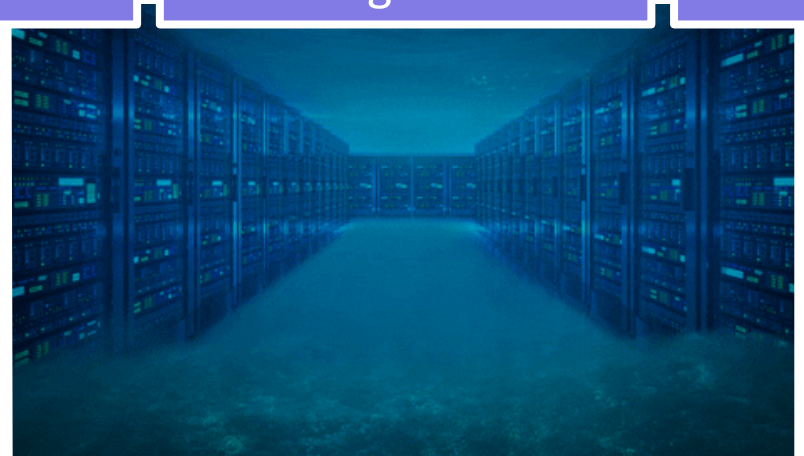
https://player.vimeo.com/video/338815600?h=08ac4da877

¡Recuerda!

La autenticación confirma una identidad de usuario comparando las credenciales recogidas en una base de datos.

Algunos métodos muy recomendables para la autenticación son:

- Uso de contraseñas
- El certificado digital
- Tarjeta inteligente
- Factores biométricos



9.3. VALIDACIÓN DE IDENTIFICACIÓN BASADA EN CLAVE SECRETA COMPARTIDA: PROTOCOLO

1

Debemos resaltar **que la validación es el paso previo a la conexión entre dos partes para establecer una clave de sesión.**

Validación de identificación basada en clave secreta compartida: protocolo

Se usa sobre todo cuando **dos usuarios comparten una clave secreta**, que ha de ser detallada a través de cualquier modo que no sea a través de internet. Es decir, esta información debería ser intercambiada en persona o por teléfono.

¿Cómo funciona?

Haz clic sobre el botón

¿Cómo funciona?

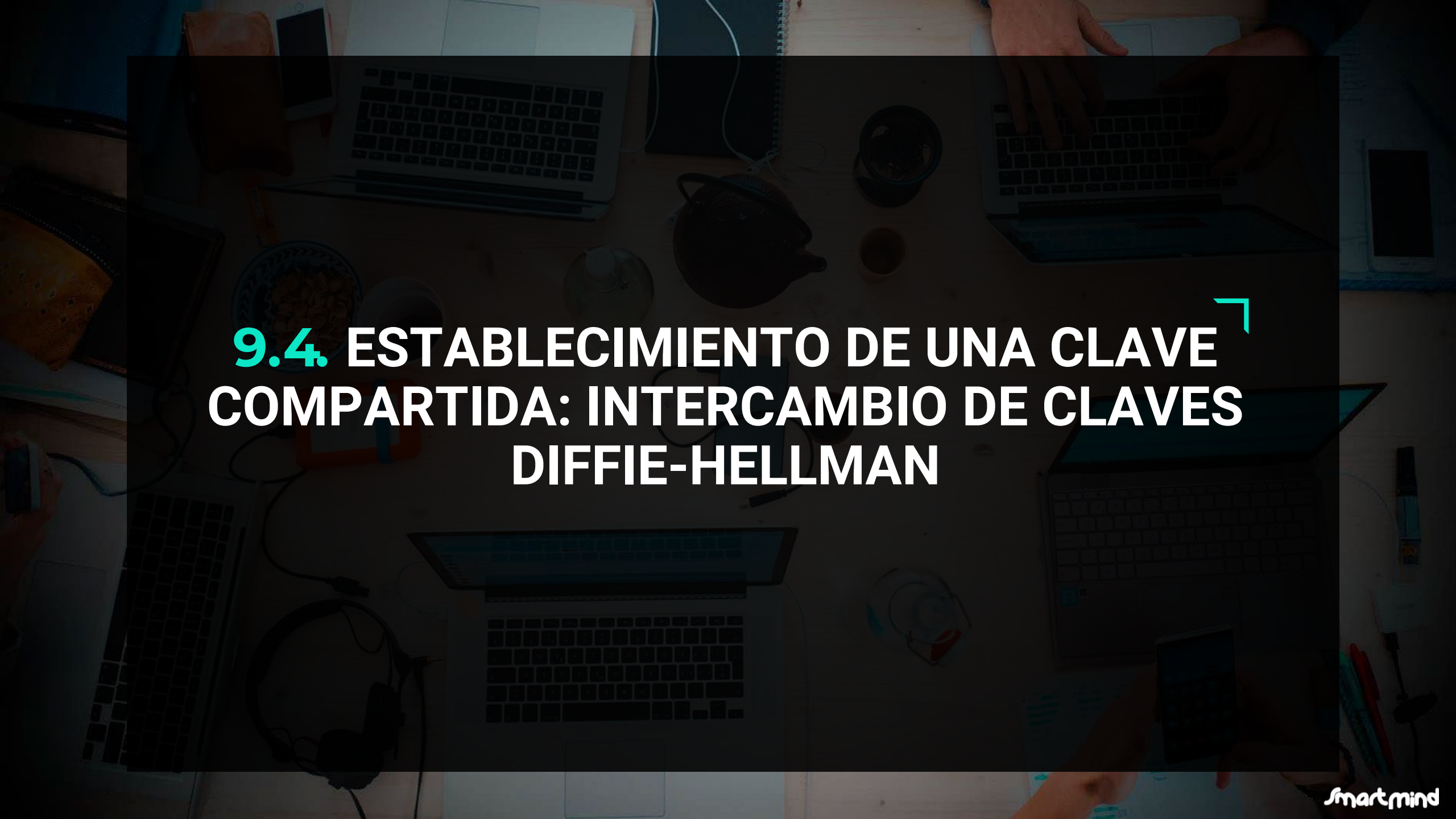
En este caso, el protocolo actúa a **modo de reto-respuesta**, que significa que **un usuario envía un número de forma totalmente aleatoria**, mientras que el otro lo transforma y devuelve el resultado al primer usuario.

R son números aleatorios grandes lanzados desde cada extremo como reto.

El paso 4 y 5 es para que A se asegure que le contesta B. Tras esta identificación, A puede indicar una **K**, para la sesión.

Este protocolo funciona, pero se puede simplificar el número de mensajes.

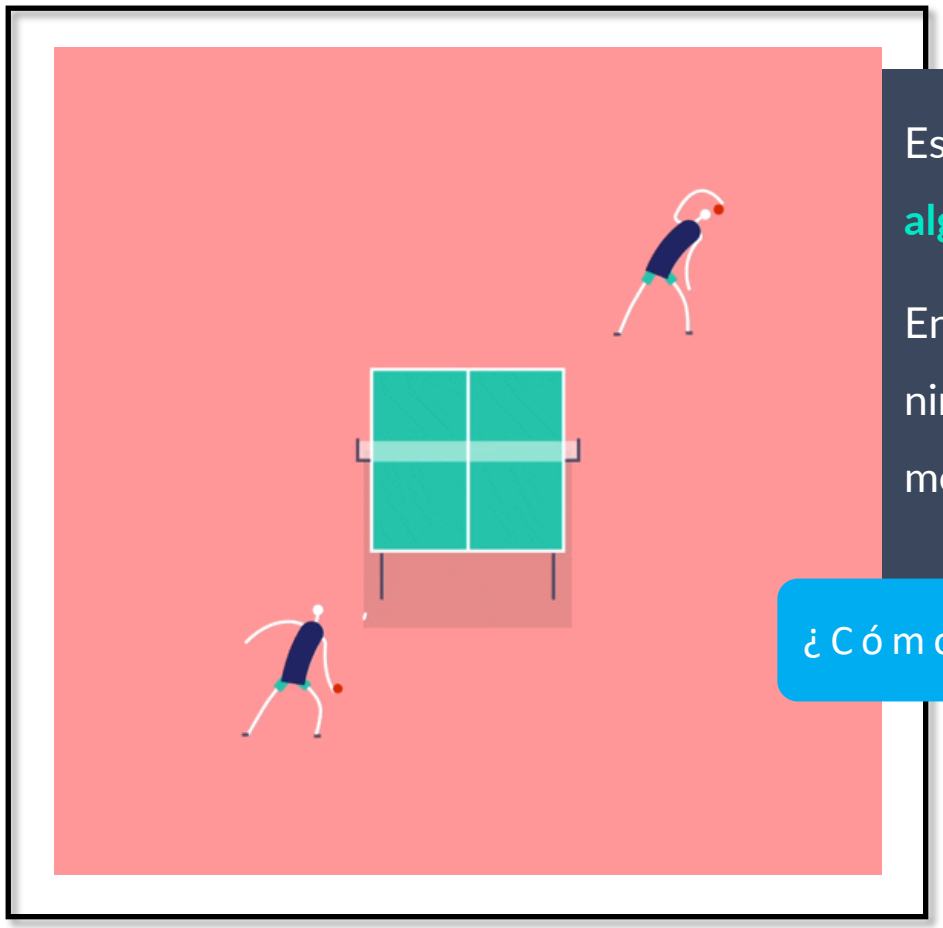
Cabe destacar que con los mensajes 2 y 3 se podría tratar intentar forzar la clave.



9.4. ESTABLECIMIENTO DE UNA CLAVE COMPARTIDA: INTERCAMBIO DE CLAVES DIFFIE-HELLMAN

2

Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman



¿Qué pasaría si se estableciese una clave secreta de forma pública?

Esto se explica con el protocolo de intercambio de Diffie-Hellman; **algoritmo de clave pública que no da opción a la autenticación.**

En este sistema, dos usuarios generan una clave compartida sin que ningún intruso pueda obtenerla aunque se encuentre en ese momento pendiente de la comunicación en sí.

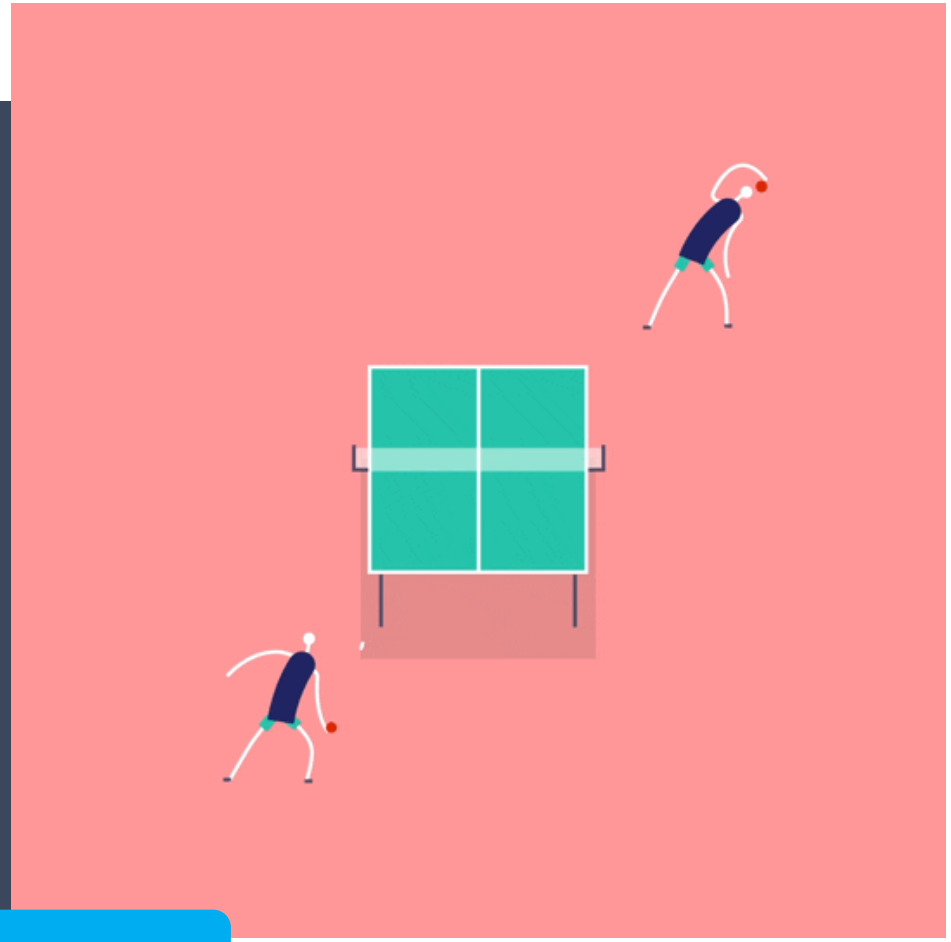
¿Cómo se pone en marcha?

Haz clic sobre el botón

¿Cómo se pone en marcha?

Se eligen dos números de forma pública y cada interlocutor escoge un número secreto. En base a una fórmula, cada uno de los usuarios (con dos números públicos y su propio número secreto) realiza unas operaciones concretas. Tras ellas, los interlocutores ponen en común sus conclusiones de forma pública.

Después, los usuarios usan, cada uno por su parte, una fórmula que lo que hace es compaginar los números que han sido transformardos junto con su número secreto. Cuando ambos llegan al final, **el resultado siempre es el mismo número que se convertirá así en la clave compartida.**



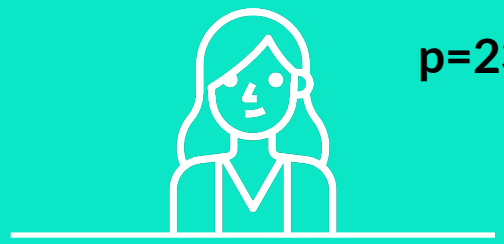
Ejemplo

Haz clic sobre el botón de ejemplo

Carlos y Alicia saben y tienen lo siguiente:

p=23 (número primo) **g=11** (un generador)

$$K = g^{ab} \bmod$$



Alicia elige un número cualquiera
a=6

Carlos elige un número cualquiera
b=5

Alicia calcula:

$A = g^a \bmod p$

$A = 11^6 \bmod 23 = 9$

Carlos calcula:

$B = g^b \bmod p$

$B = 11^5 \bmod 23 = 5$

Alicia recibe **B=5** de Carlos

Carlos recibe **B=9** de Alicia

Llave secreta:

$K = B^a \bmod p$

$K = 5^6 \bmod 23$

$K = 8$

La clave conjunta secreta será **8**

Llave secreta:

$K = A^b \bmod p$

$K = 9^5 \bmod 23$

$K = 8$

9.5. VALIDACIÓN DE IDENTIFICACIÓN USANDO UN CENTRO DE DISTRIBUCIÓN DE CLAVES

3

Validación de identificación usando un centro de distribución de claves: KDC (Key Distribution Center)

También existe la posibilidad de usar un centro de distribución de claves fiables, reconocido por sus siglas KDC (Key Distribution Center). **En este protocolo, cada usuario tiene una clave que comparte con el centro, por el que ha de pasar la validación de identificación y administración de claves.**

Característica principal

La característica principal de la KDC es que **crea una clave secreta para cada uno de los miembros, pero que solo puede ser utilizada entre el miembro y el centro, no entre los miembros.**

Objetivo

Su principal objetivo es el de **reducir de forma considerable los riesgos que suelen generarse debido al intercambio de claves.**

KDC. Utilizar técnicas criptográficas

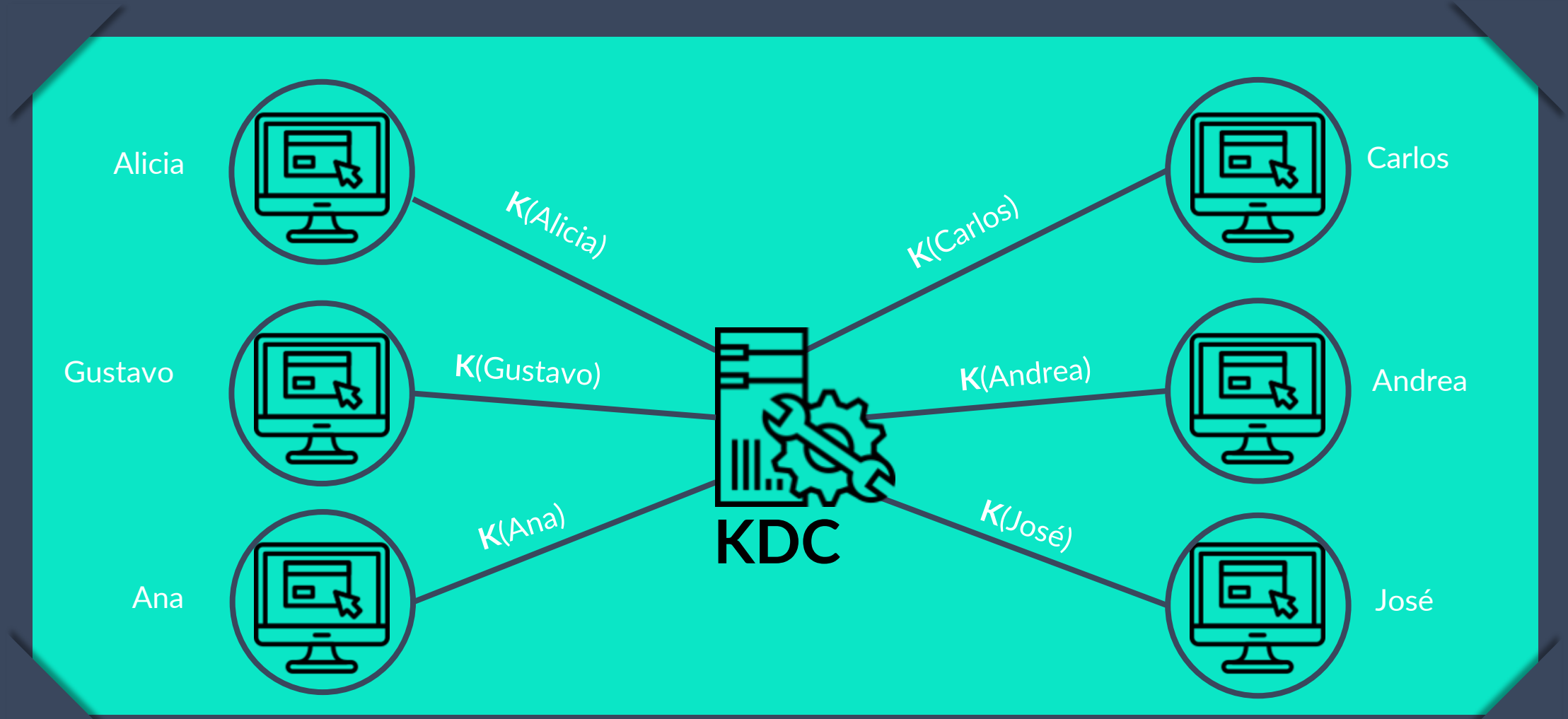
- Autenticar a los usuarios
- Verificar si pueden o no acceder a lo que solicitan
- Ver si cumplen con las condiciones

Esto significa que el KDC **se encarga de verificar que los usuarios cuentan con el derecho a acceder a la comunicación y determina su paso.**

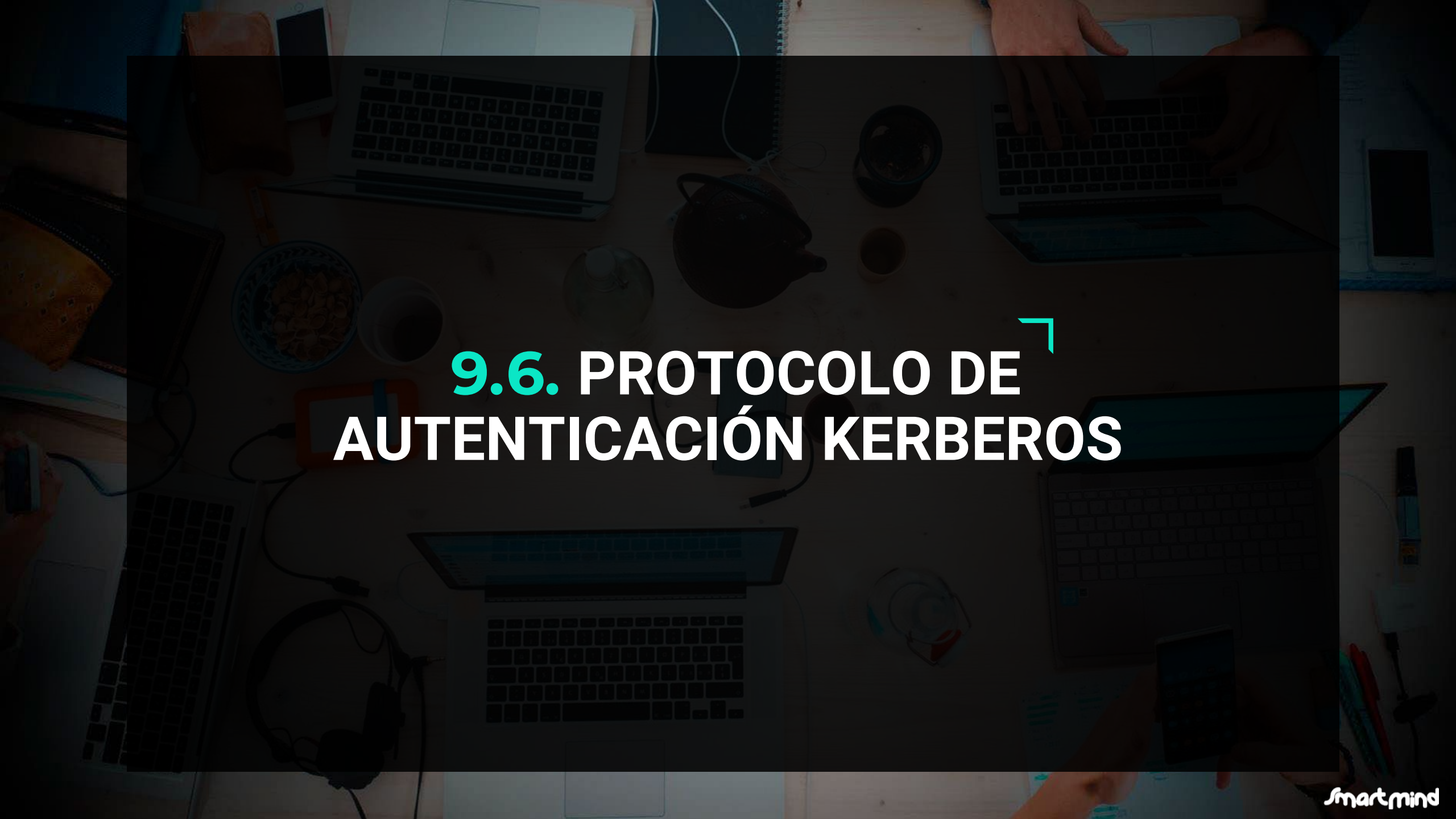
Los KDC son, la mayoría de las veces, de cifrado simétrico y comparten clave con las otras partes.

¿Cómo se utiliza?

Haz clic en el botón



Cada uno de los usuarios cuenta con una clave única que comparten con el KDC, el cual se encarga de validarla.



9.6. PROTOCOLO DE AUTENTICACIÓN KERBEROS

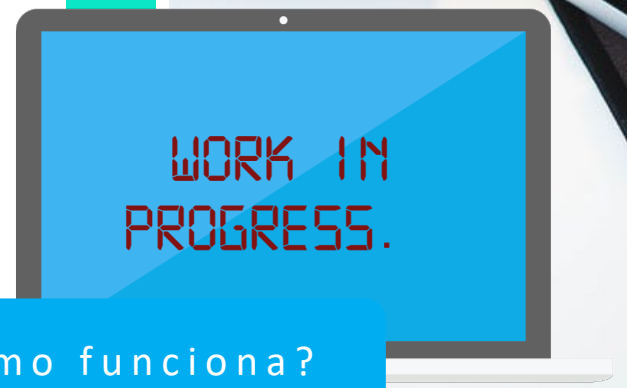
4

Protocolo de autenticación de Kerberos

El Protocolo de Autenticación de Kerberos es un servicio de validación de identificación desarrollado en el MIT (Massachusetts Institute of Technology).

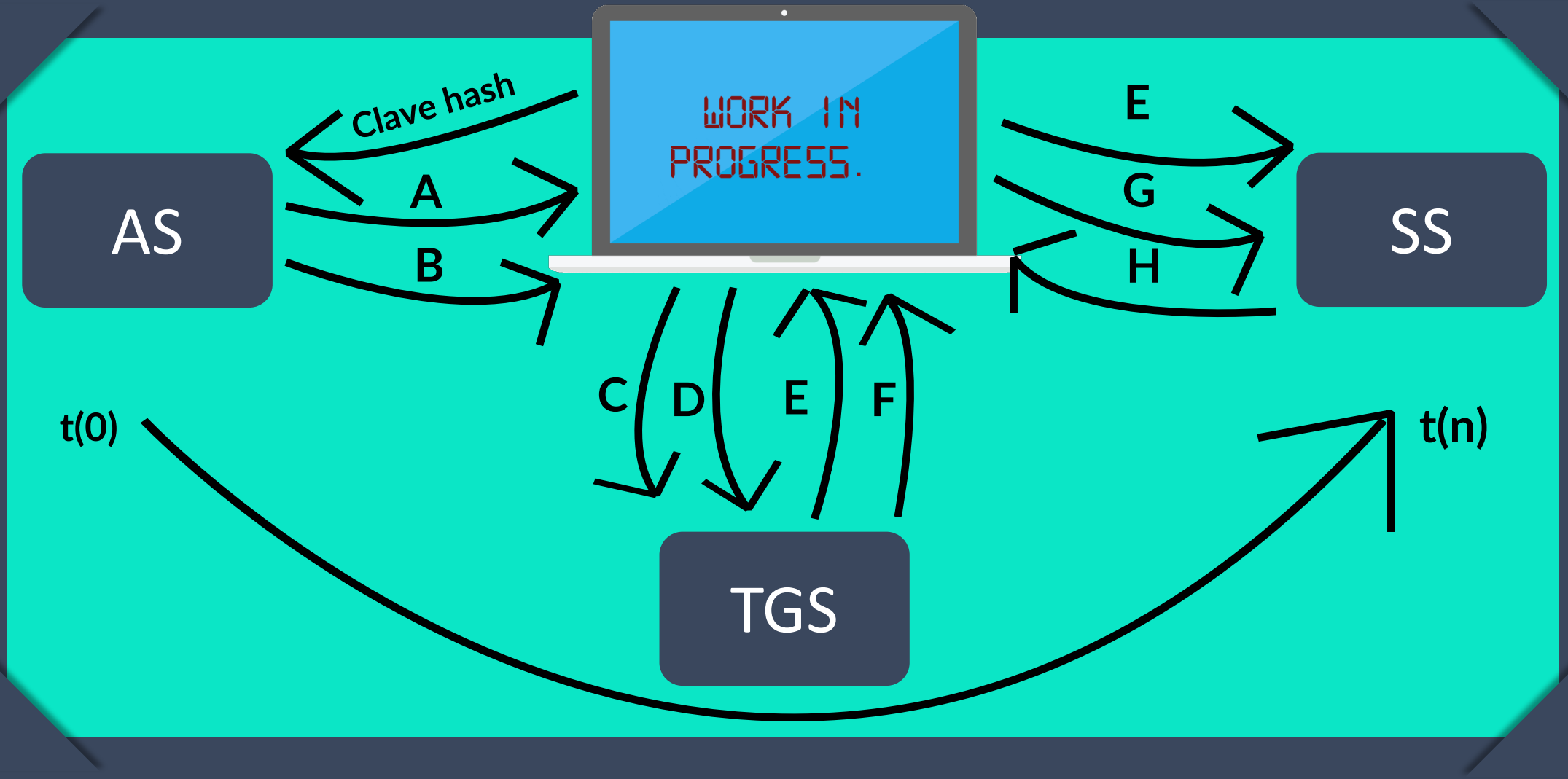
Este da la opción a dos ordenadores de mostrar su identidad de forma segura en una red insegura. Su origen lo encontramos en el modelo cliente-servidor, que ofrece una autenticación mutua, en la que el cliente y el servidor verifican la identidad del otro.

Necesita a un tercero que le ofrezca seguridad. Vendría a ser algo así como un árbitro en el que recae la confianza de los usuarios y que ofrece a cada uno de ellos una clave secreta diferente. El hecho de conocer la clave es usado como una prueba de identificación.



¿Cómo funciona?

Haz clic sobre el botón



El objetivo principal de este protocolo es autenticar al cliente contra el “Servidor de Autenticación” (AS), de forma que así lo pueda demostrar frente al “Servidor de concesión de tickets” (TGS) y recibir un ticket de servicio. Una vez finalizado este proceso, podrá demostrar al “Servidor de Servicio” (SS) que ha pasado las “pruebas” y que está aprobado para utilizar el servicio de Kerberos.

9.7. VALIDACIÓN DE IDENTICACIÓN DE CLAVE PÚBLICA

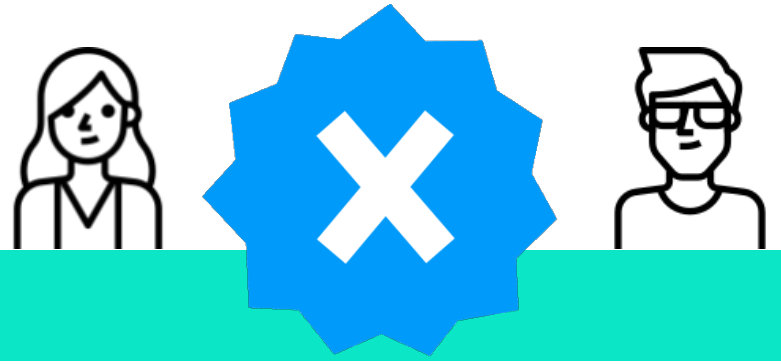
1

Validación de identificación de clave pública.

En el supuesto de que **los usuarios A y B conozcan previamente las claves públicas del otro**, establecerán una sesión en la que hagan uso de la criptografía de clave secreta, la cual es considerablemente más rápida.

En un primer lugar, tendrán que validar la identificación de ambos usuarios con claves públicas que sirvan para comunicarse y las privadas para descifrar. Tras ello, se acuerda una clave secreta compartida.

En este caso, un intruso no podría entrar en la comunicación, a no ser que haya algún problema en el proceso de intercambio de las claves públicas.



Si **los usuarios A y B, por el contrario, no conocen la clave pública del otro**, el primer usuario tendría que mandar su clave pública al segundo y solicitarle la suya.

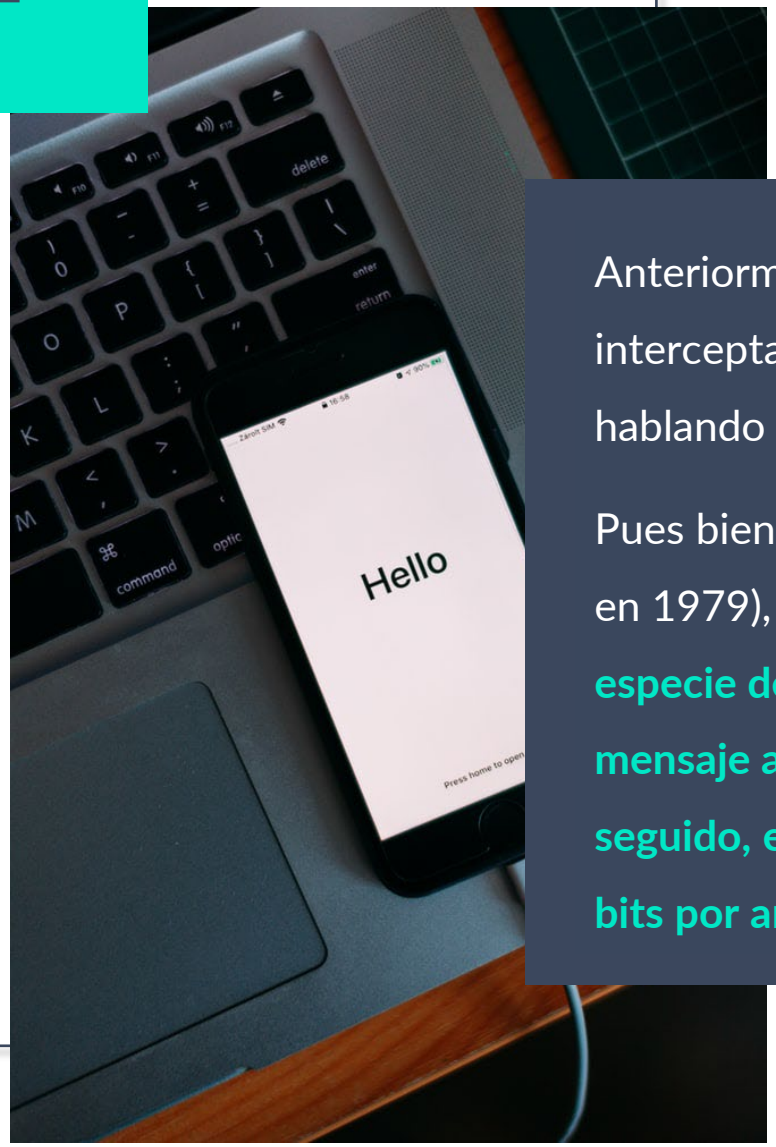
Sin embargo, esto tiene un pequeño impedimento y es que necesita de alguien que haga de intermediario o basarlo en un ataque de brigada de cubetas.

Este método permite al “interceptor” coger el mensaje y devolver su clave al primer usuario, para que este piense que está hablando con el segundo usuario, cuando realmente lo está haciendo con el intermediario.

De esta forma, el “tercero” puede leer los mensajes cifrados.

9.8. VALIDACIÓN DE IDENTICACIÓN DE CLAVE PÚBLICA: PROTOCOLO DE INTERBLOQUEO

2



Protocolo de interbloqueo

Anteriormente hablábamos del “ataque de brigada de cubetas” como una forma de interceptar el mensaje y devolver una clave al primer usuario para que piense que está hablando con el usuario al que mandó su mensaje.

Pues bien, Rivest y Shamir, del RSA (sistema criptográfico de clave pública desarrollado en 1979), diseñaron un protocolo que impedía este ataque. **En este caso, se realiza un especie de “interbloqueo”, en el que el primer usuario solo manda la mitad del mensaje al segundo, que responde con el resto de bits del mensaje encriptado. Acto seguido, el primero manda el resto de bits y el segundo los suyos hasta completar los bits por ambas partes.**

Todo esto significa que en el caso de que alguno de los usuarios no realice correctamente la entrega de sus bits, **el protocolo automáticamente fallará.**

Además, si el intermediario recibe alguna de las tandas de los bits no podrá hacer nada con ellos, puesto que le faltará la otra mitad para entender algo y poder descifrarlo. **Esto quiere decir que no podrá volver a cifrarlo usando la clave pública del segundo usuario y que si prueba a mandar algo lo más probable es que no tenga sentido y que el engaño sea fácilmente reconocible.**


¡Enhorabuena!
¡Has conseguido superar la última unidad!
smartmind